ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 22080—2008/ISO/IEC 27001:2005

# 信息技术　安全技术
# 信息安全管理体系　要求

**Information technology—Security techniques—**
**Information security management systems—Requirements**

(ISO/IEC 27001:2005, IDT)

2008-06-19 发布　　2008-11-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

# 目　　次

# 前　言

本标准等同采用 ISO/IEC 27001:2005《信息技术　安全技术　信息安全管理体系　要求》，仅有编辑性修改。

本标准的附录 A 是规范性附录，附录 B 和附录 C 是资料性附录。

本标准由中华人民共和国信息产业部提出。

本标准由全国信息安全标准化技术委员会归口。

本标准由中国电子技术标准化研究所、上海三零卫士有限公司、北京知识安全工程中心、北京市信息安全测评中心、北京数字认证中心负责起草。

本标准主要起草人：上官晓丽、许玉娜、胡啸、王新杰、赵战生、王连强、曾波、孔一童、刘海峰、汤永利、尚小鹏、闵京华。

# 引　言

## 0.1　总则

本标准用于为建立、实施、运行、监视、评审、保持和改进信息安全管理体系(Information Security Management System,简称 ISMS)提供模型。采用 ISMS 应当是一个组织的一项战略性决策。一个组织 ISMS 的设计和实施受其需要和目标、安全要求、所采用的过程以及组织的规模和结构的影响,上述因素及其支持系统会不断发生变化。按照组织的需要实施 ISMS 是本标准所期望的,例如,简单的情况可采用简单的 ISMS 解决方案。

本标准可被内部和外部相关方用于一致性评估。

## 0.2　过程方法

本标准采用过程方法来建立、实施、运行、监视、评审、保持和改进组织的 ISMS。

为使组织有效运作,需要识别和管理众多相互关联的活动。通过使用资源和管理,将输入转化为输出的活动可视为过程。通常,一个过程的输出直接形成下一个过程的输入。

组织内诸过程的系统的应用,连同这些过程的识别和相互作用及其管理,可称之为"过程方法"。

本标准中提出的用于信息安全管理的过程方法鼓励其用户强调以下方面的重要性:

a)　理解组织的信息安全要求和建立信息安全方针与目标的需要;

b)　从组织整体业务风险的角度,实施和运行控制措施,以管理组织的信息安全风险;

c)　监视和评审 ISMS 的执行情况和有效性;

d)　基于客观测量的持续改进。

本标准采用了"规划(Plan)—实施(Do)—检查(Check)—处置(Act)"(PDCA)模型,该模型可应用于所有的 ISMS 过程。图 1 说明了 ISMS 如何把相关方的信息安全要求和期望作为输入,并通过必要的行动和过程,产生满足这些要求和期望的信息安全结果。图 1 也描述了第 4 章、第 5 章、第 6 章、第 7 章和第 8 章所提出的过程间的联系。

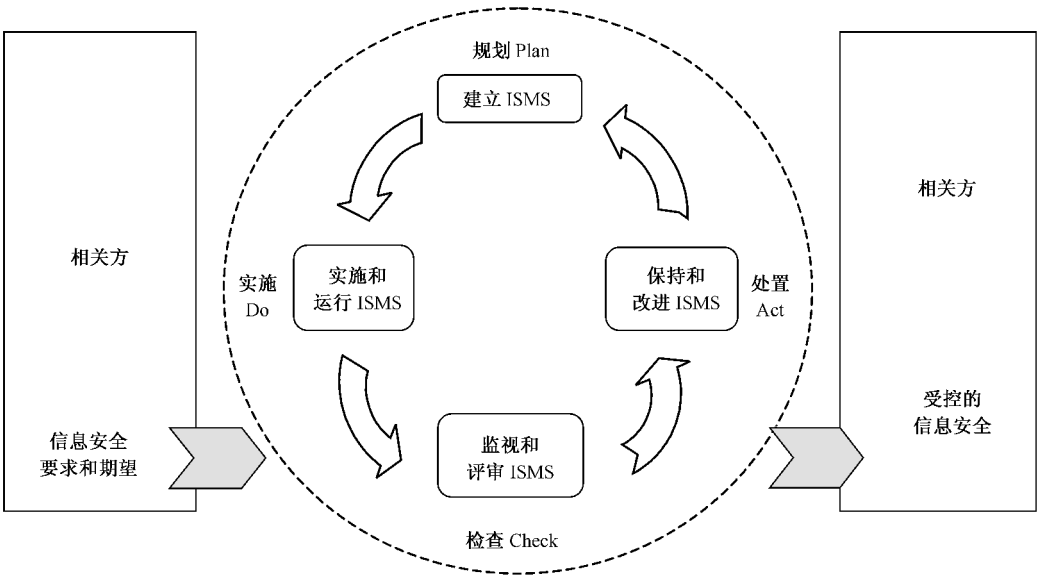


**图 1　应用于 ISMS 过程的 PDCA 模型**

采用 PDCA 模型还反映了治理信息系统和网络安全的 OECD 指南(2002 版)[1] 中所设置的原则。本标准为实施 OECD 指南中规定的风险评估、安全设计和实施、安全管理和再评估的原则提供了一个强健的模型。

例 1:某些信息安全违规不至于给组织造成严重的财务损失和/或使组织陷入困境。这可能是一种要求。

例 2:如果发生了严重的事件(可能是组织的电子商务网站被黑客入侵)应有经充分培训的员工按照适当的规程,将事件的影响降至最小。这可能是一种期望。

| | |
|---|---|
| 规划(建立 ISMS) | 建立与管理风险和改进信息安全有关的 ISMS 方针、目标、过程和规程,以提供与组织总方针和总目标相一致的结果。 |
| 实施(实施和运行 ISMS) | 实施和运行 ISMS 方针、控制措施、过程和规程。 |
| 检查(监视和评审 ISMS) | 对照 ISMS 方针、目标和实践经验,评估并在适当时测量过程的执行情况,并将结果报告管理者以供评审。 |
| 处置(保持和改进 ISMS) | 基于 ISMS 内部审核和管理评审的结果或者其他相关信息,采取纠正和预防措施,以持续改进 ISMS。 |

## 0.3 与其他管理体系的兼容性

本标准与 GB/T 19001—2000 及 GB/T 24001—2004 相结合,以支持与相关管理标准一致的、整合的实施和运行。因此,一个设计恰当的管理体系可以满足所有这些标准的要求。表 C.1 说明了本标准、GB/T 19001—2000 和 GB/T 24001—2004 的各条款之间的关系。

本标准的设计能够使一个组织将其 ISMS 与其他相关的管理体系要求结合或整合起来。

1) OECD 信息系统和网络安全指南——面向安全文化。巴黎:OECD,2002 年 7 月。www.oecd.org

# 信息技术　安全技术
# 信息安全管理体系　要求

**重要提示:本出版物不声称包括一个合同所有必要的条款。用户负责对其进行正确的应用。符合标准本身并不获得法律责任的豁免。**

## 1　范围

### 1.1　总则

本标准适用于所有类型的组织(例如,商业企业、政府机构、非赢利组织)。本标准从组织的整体业务风险的角度,为建立、实施、运行、监视、评审、保持和改进文件化的信息安全管理体系(ISMS)规定了要求。它规定了为适应不同组织或其部门的需要而定制的安全控制措施的实施要求。

ISMS 的设计应确保选择适当和相宜的安全控制措施,以充分保护信息资产并给予相关方信心。

注 1:本标准中的"业务"一词应广义的解释为关系一个组织生存的核心活动。

注 2:GB/T 22081—2008 提供了设计控制措施时可使用的实施指南。

### 1.2　应用

本标准规定的要求是通用的,适用于各种类型、规模和特性的组织。组织声称符合本标准时,对于第 4 章、第 5 章、第 6 章、第 7 章和第 8 章的要求不能删减。

为了满足风险接受准则必要的进行的任何控制措施的删减,必须证明是合理的,且需要提供证据证明相关风险已被负责人员接受。除非删减不影响组织满足由风险评估和适用法律法规要求所确定的安全要求的能力和/或责任,否则不能声称符合本标准。

注:如果一个组织已经有一个运转着的业务过程管理体系(例如,与 GB/T 19001—2000 或者 GB/T 24001—2004 相关的),那么在大多数情况下,更可取的是在这个现有的管理体系内满足本标准的要求。

## 2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB/T 22081—2008　信息技术　安全技术　信息安全管理实用规则(ISO/IEC 27002:2005,IDT)

## 3　术语和定义

下列术语和定义适用于本标准。

3.1

**资产　asset**

对组织有价值的任何东西。

[ISO/IEC 13335-1:2004]

3.2

**可用性　availability**

根据授权实体的要求可访问和利用的特性。

[ISO/IEC 13335-1:2004]

3.3

**保密性　confidentiality**

信息不能被未授权的个人、实体或者过程利用或知悉的特性。